Handling SNMP Traps Using eG Enterprise

Handling SNMP Traps Using eG Enterprise

SNMP traps are used to asynchronously send real-time network error messages for any object registered on the network to an SNMP Manager.

Whenever an SNMP agent detects an error in an SNMP-enabled network device / application, it sends SNMP traps with the error information to a daemon process known as the SNMP Trap Receiver (Snmptrapd). In the eG Enterprise system, the external agent includes an optional SNMP trap receiver that can log traps it receives into a log file which can be parsed/interpreted by the external agent.

This chapter explains the procedures involved in setting up SNMP trap daemon on Linux, Solaris, and Windows systems, and also discusses how the eG agents integrate with the Snmptrapd to retrieve critical performance metrics.

1.1 Configuring Snmptrapd on Linux Systems

To setup Snmptrapd on Linux, do the following:

1. Key shell scripts essential for Snmptrapd configuration are bundled with the eG agent package for Linux. Installing the eG agent therefore, will automatically create the **/opt/egurkha/agent/snmptrapd** directory containing the **check_trapd**, **start_trapd**, and **cron_trapd** files and a sub-directory named **log**.
2. Next, execute the shell script defined within the **cron_trapd** file by issuing the command **crontab cron_trapd** from the **/opt/egurkha/agent/snmptrapd** directory. This command will invoke the **check_trapd** script.

> **Note:**
>
> If the **SetUI operation not permitted** error appears while executing the **crontab cron_trapd** command, do the following:
>
> - Verify whether the root-user is the owner of **crontab**. If not, issue the command - **chown root:root crontab** - to change the ownership of **crontab**.
> - Then, execute the command: **chmod +s crontab** to give the appropriate execution privileges to the user running the **crontab** command. .

3. The primary responsibility of the **check_trapd** script is to start the Snmptrapd process using the **start_trapd** file. Additionally, the **check_trapd** will check if the **snmptrapd.log** file has reached a size of 1MB. If so, it will delete the file and restart the Snmptrapd process so as to prevent the log from growing excessively.
4. The **start_trapd** file will contain the port at which the Snmptrapd process listens for SNMP traps from SNMP agents. The default SNMP trap port is 162. However, in Unix environments, a default Snmptrapd process already runs at this port. Therefore, for Unix environments, the port has been set to 6667. This default port setting can be modified by editing the **port** parameter of the **start_trapd** file.

Note:

Ensure that the port number and community string (default: public) specified in the **start_trapd** file is the same as the SNMP port of the application or network device from which the SNMP traps originate.

1.2 Configuring Snmptrapd on Solaris

To setup Snmptrapd on Solaris, do the following:

1. In Solaris, the Snmptrapd package comes bundled along with the eG agent package. Therefore, first, install the eG agent.
2. Upon agent installation, the **/opt/egurkha/agent/snmptrapd** directory will be automatically created. This directory will contain the files **check_trapd**, **start_trapd**, and **cron_trapd**, and a sub-directoy named **log**.
3. To start the Snmptrapd process, execute the command **crontab cron_trapd** from the **/opt/egurkha/agent/snmptrapd** directory.
4. The **start_trapd** file will contain the port at which the Snmptrapd process listens for SNMP traps from SNMP agents. The default SNMP trap port is 162. However, in Solaris environments, a default Snmptrapd process already runs at this port. Therefore, for Unix environments, the port has been set to 6667. This default port setting can be modified by editing the **port** parameter of the **start_trapd** file.

Note:

Ensure that the port number and community string (default: *public*) specified in the **start_trapd** file is the same as the SNMP port of the application or network device from which the SNMP traps originate.

1.3 Configuring Snmptrapd on Windows

In Windows environments too, the Snmptrapd package comes bundled with the eG agent package. To setup Snmptrapd on Windows, do the following:

1. Install the eG agent. This will create the **snmptrapd** directory under the **<EG_INSTALL_DIR>\agent** directory.
2. From the command prompt, switch to the **<EG_INSTALL_DIR>\agent \snmptrapd** directory, and execute the **runTrapd.bat** batch file to register the Snmptrapd as a service in Windows.
3. By default, snmptrapd will run on port 162 and will use the community string *public*. To have the SNMP daemon use a different port, edit the **runTrapd.bat** file and change the default port number 162 in the **-p 162** specification of the file (indicated by Figure 1) to reflect a port of your choice. Similarly, you can change the default **–c public** specification in the file to reflect the community string that snmptrapd should use in your environment.

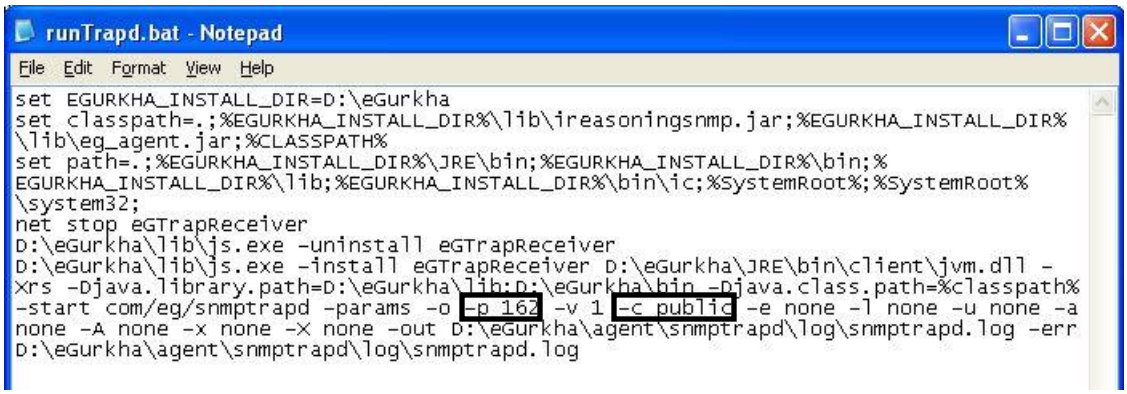

Figure 1: Default port number and community string

4. Finally, start the Snmptrapd process by right-clicking on the **eG Trap Receiver** in the **Services** window (Start -> Programs -> Administrative Tools -> Services), and selecting the **Start** option from its shortcut menu.

Note:

- Ensure that the port number and community string (default: *public*) specified in the **runTrapd.bat** file is the same as the SNMP port of the application or network device from which the SNMP traps originate.
- To unregister the Snmptrapd service, run the **unregistertrapd.bat** file from the **<EG_INSTALL_DIR>\agent \snmptrapd** directory.
- To change the configuration for the Snmptrapd log file size, modify the **traploglength** parameter in the **eg_counter.ini** file in the **<EG_INSTALL_DIR>\agent\config** directory.
- To configure the SNMP Trap Receiver with SNMP v3 support, follow the steps discussed below:
  - Edit the **runtrapd.bat** file in the **<EG_INSTALL_DIR>\agent \snmptrapd** directory.
  - Ensure that **-v** parameter is set to *3* to support SNMP version 3. Also, since SNMP v3 does not support a community string, make sure that the **-c** parameter is set to *none*.
  - Then, ensure that valid values are provided for the following parameters in the **runtrapd.bat** file:

Parameter	Value
-e	Engine ID
-l	Security level; this can be **noAuthNoPriv**, **authNoPriv**, or **authPriv**
-u	Security name or user name
-a	Authentication protocol; this can be **MD5** (for Message Digest Algorithm) or **SHA** (for Secure Hash Algorithm)
-A	Authentication protocol pass phrase
-x	Privacy protocol; this can be **DES** (for Data Encryption Standard)
-X	Privacy protocol pass phrase

A sample entry has been provided below:

-p 162 -v 3 -c none -e 80.00.08.1c.04.46.64 -l authNoPriv -u Kevin -a MD5 -A kvn1234 -x DES -X kvn12345

- Finally, save the file.

1.4 Administering the eG Manager to Display Information on SNMP Traps

1. Login to eG administrative interface as *admin*. To display trap messages, eG uses two tests, namely, Network Traps test and Application Traps test. While the Application Traps test is associated with the **Application Processes** layer, the Network Traps test is associated with the **Network** layer. The Network Traps test is an external test that reports the count of SNMP trap messages received from network devices. The Application Traps test test, also executed by an external agent, reports the number of SNMP trap messages sent by applications. These tests have been mapped to the *Network node* and *Cisco router* components. Therefore, to configure these tests, first manage a component of type *Network Node* or *Cisco Router*.
2. Then, open the **ENABE / DISABLE TESTS** page using the menu sequence: Agents -> Tests -> Enable / Disable menu sequence. Select the component type to which the tests have been associated from the list box therein, pick **Performance** as test type, pick the **Network Traps** test from the **DISABLED TESTS** list, click the **>>** button to move it to the **ENABLED TESTS** list, and finally click on the **Update** button to save the changes.
3. Then, proceed to configure the test for a specific component by navigating to the **SPECIFIC CONFIGURATION** page (Agents -> Tests -> Specific Configuration). Doing so will open Figure 2 using which the test can be configured.

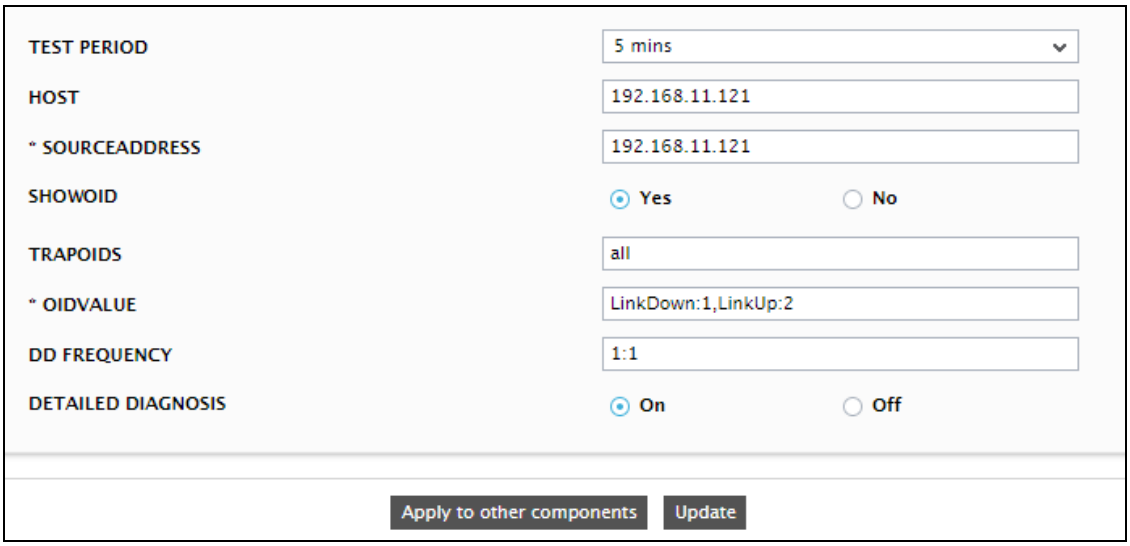

Figure 2: Configuring the Network Traps test

4. In Figure 2, specify the following:
   - **TEST PERIOD** - How often should the test be executed
   - **HOST** - The host for which the test is to be configured

- **SOURCEADDRESS** - Specify a comma-separated list of IP addresses or address patterns of the hosts from which traps are considered in this test. For example, *10.0.0.1,192.168.10.**. A leading '*' signifies any number of leading characters, while a trailing '*' signifies any number of trailing characters.

- **OIDVALUE** - Provide a comma-separated list of OID and value pairs returned by the traps. The values are to be expressed in the form, *DisplayName:OID-OIDValue*. For example, assume that the following OIDs are to be considered by this test: *.1.3.6.1.4.1.9156.1.1.2* and *.1.3.6.1.4.1.9156.1.1.3*. The values of these OIDs are as given hereunder:

OID	Value
.1.3.6.1.4.1.9156.1.1.2	Host_system
.1.3.6.1.4.1.9156.1.1.3	NETWORK

  In this case the oidvalue parameter can be configured as *Trap1:.1.3.6.1.4.1.9156.1.1.2-Host_system,Trap2:.1.3.6.1.4.1.9156.1.1.3-Network*, where *Trap1* and *Trap2* are the display names that appear as descriptors of this test in the monitor interface.

  An * can be used in the OID/value patterns to denote any number of leading or trailing characters (as the case may be). For example, to monitor all the OIDs that return values which begin with the letter 'F', set this parameter to *Failed:*-F**.

  Typically, if a valid value is specified for an OID in the *OID-value* pair configured, then the test considers the configured OID for monitoring only when the actual value of the OID matches with its configured value. For instance, in the example above, if the value of OID *.1.3.6.1.4.1.9156.1.1.2* is found to be *HOST* and not *Host_*system, then the test ignores OID *.1.3.6.1.4.1.9156.1.1.2* while monitoring. In some cases however, an OID might not be associated with a separate value – instead, the OID itself might represent a value. While configuring such OIDs for monitoring, your oidvalue specification should be: *DisplayName:OID-any*. For instance, to ensure that the test monitors the OID *.1.3.6.1.4.1.9156.1.1.5*, which in itself, say represents a failure condition, then your specification would be:

  Trap5: .1.3.6.1.4.1.9156.1.1.5-any.

- **SHOWOID** – Specifying **true** against **SHOWOID** will ensure that the detailed diagnosis of this test shows the OID strings along with their corresponding values. If you enter **false**, then the values alone will appear in the detailed diagnosis page, and not the OIDs.

- **TRAPOIDS** – By default, this parameter is set to *all*, indicating that the eG agent considers all the traps received from the specified sourceaddresses. To make sure that the agent considers only specific traps received from the sourceaddress, then provide a comma-separated list of OIDs in the trapoids text box. A series of OID patterns can also be specified here, so that the test considers only those OIDs that match the specified pattern(s). For instance, ***94.2**,*.1.3.6.1.4.25**, where * indicates leading and/or trailing spaces.

- **DD FREQUENCY** - Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against dd frequency.

- **DETAILED DIAGNOSIS** - To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the

capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:

- The eG manager license should allow the detailed diagnosis capability
- Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

5. Finally, click the **Update** button in Figure 2.
6. Similarly, the Application Traps test can also be configured. Then, signout of the administrative interface.

1.5 Monitoring SNMP Traps

To view the measures pertaining to SNMP traps, do the following:

1. Login to the eG monitor interface as *supermonitor*.
2. Follow the Hosts/Applications -> Components menu sequence.
3. From the **COMPONENT LIST** page that appears, click on the component to which the Network Traps test or Application Traps test is mapped. Figure 3 will then appear.

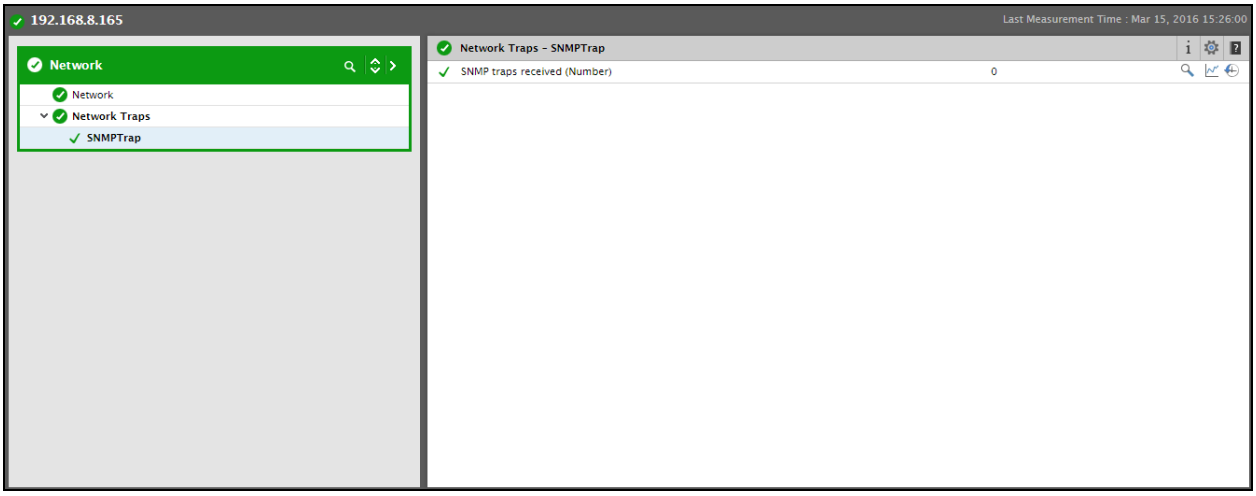

Figure 3: Measures pertaining to Network Traps test

4. If detailed diagnosis has been enabled for the test, then click on the 'magnifying glass' icon against the measure name in Figure 3. This will reveal the details reported by the SNMP agent via traps – the details include the time at which the SNMP trap was received, the IP address of the trap sender, the trap type, and the contents of the trap. If the **SHOWOID** parameter is set to **true**, then the contents of the trap (i.e., the **Trap Details** column) will display the OID and its value (see Figure 4). If the flag is set to **false** instead, only the values will be displayed in the **Trap details** column and not the OIDs.

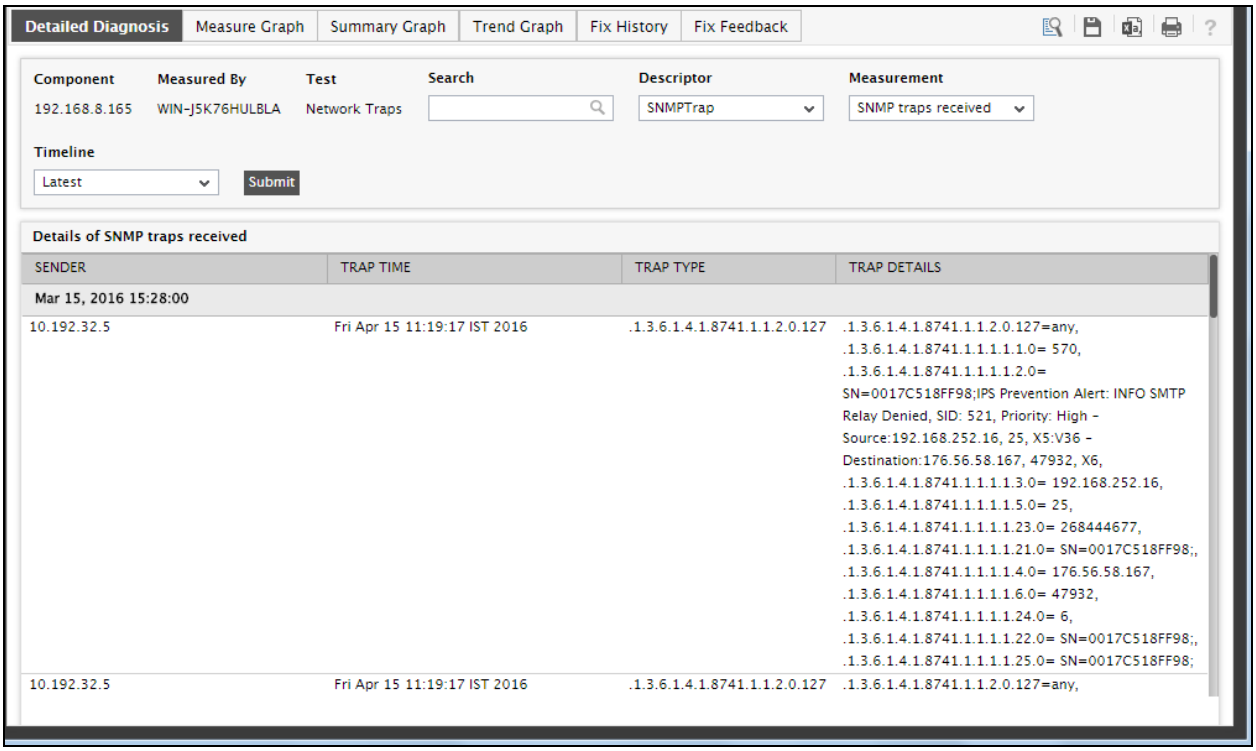

Figure 4: The detailed diagnosis of the NetworkTraps test

Note:

For more clarity, you might want the OIDs displayed in the detailed diagnosis to be replaced by their corresponding object names. To ensure this, you first need to upload the SNMP MIB files of all those applications/devices from which traps are to be received, to the eG manager. The procedure for uploading MIB files to the eG manager is detailed in Section 1.6 below.

After the upload is complete, do the following:

1. Edit the **eg_external.ini** file in the **<EG_INSTALL_DIR>\manager\config** directory.
2. In the **[MISC]** section of the file, set the **ExpandMib** flag to **true**.
3. Then, make sure that the tests reporting the trap details are available in the **[SNMP_Tests]** section of the file. If not, enter the 'internal names' of these tests in that section. For instance, to ensure that the detailed diagnosis of the NetworkTraps test and the ApplicationTraps test converts OIDs into corresponding object names, include the internal names of these two tests – i.e., *NetworkTrapTest* and *AppTrapTest* – in the **[SNMP_Tests]** section in the following format:

```
[SNMP_Tests]

NetworkTrapTest=yes
AppTrapTest=yes
```

   To know the internal test names, refer to the **eg_lang*.ini** file in the **<EG_INSTALL_DIR>\manager\config**, where * is the language code that represents the language preference that you have set using the **USER PROFILE** page. In this file, the component types, measure names, test names, layer names, measure descriptions, and a wide range of other display information are expressed in a particular language, and are mapped to their eG equivalents. Search the file for the test of interest to you. For instance, to know the internal name for the *Processes* test, search the **[TEST_NAME_MAPPING]** section of the file for *Processes*. This will reveal the internal test name that maps to Processes.

4. Finally, save the file.

1.6 Uploading SNMP MIB Files

By default, tests that monitor the SNMP traps received by the eG manager, display only the OIDs contained within the traps in their detailed diagnosis. Sometimes, for want of clarity, administrators might prefer to include the object names in the detailed diagnosis instead of the OIDs. The first step towards ensuring this is to upload to the eG manager the SNMP MIB files that correspond to the sources of these SNMP traps; these MIB files typically, bear the OID-object name mappings.

In order to enable administrators to upload MIB files, the eG administrative interface provides a **DELETE AND UPLOAD MIB FILES** page. To access this page, use the *Alerts -> SNMP Traps -> Upload MIB* menu sequence. To upload MIB files using this page, do the following:

1. If no MIB files have been uploaded to the eG manager yet, then the message depicted by Figure 5 will be

displayed in the **DELETE AND UPLOAD MIB FILES** page.

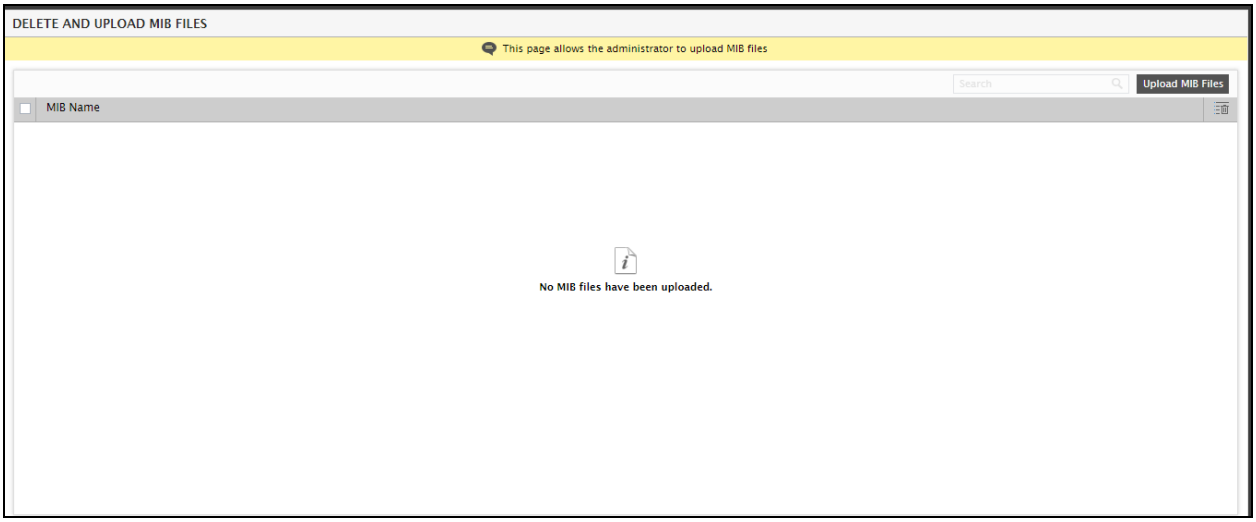

Figure 5: The DELETE AND UPLOAD MIB FILES page indicating that no MIB files are currently available

2. To upload a MIB file, first click on the **Upload MIB Files** button at the right top corner of Figure 5.
3. Figure 6 will then appear, where you can specify the full path to the MIB file to be uploaded. The **Browse** button in Figure 6 can be used for quickly locating the MIB file.

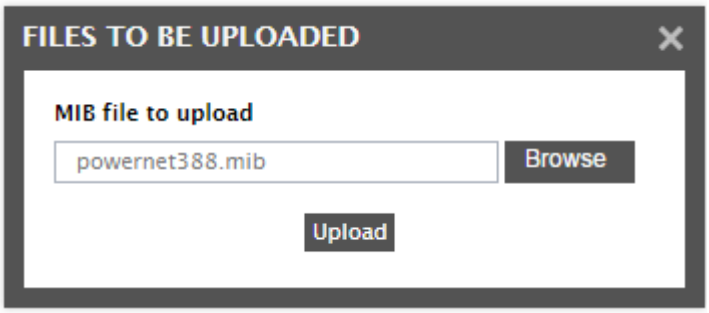

Figure 6: Specifying the full path to the MIB file to be uploaded

4. Then, click the **Upload** button in Figure 6.
5. If upload is successful, you will return to the **DELETE AND UPLOAD MIB FILES** page, where the newly uploaded file will be listed.

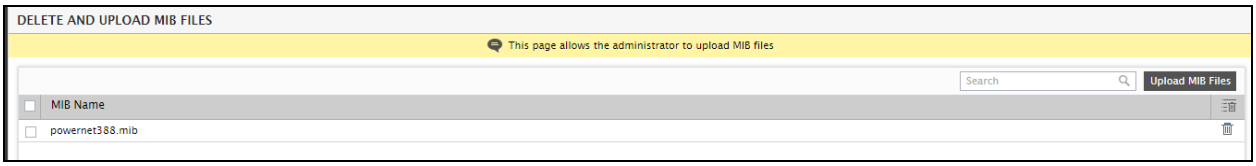

Figure 7: The MIB file newly uploaded displayed in the DELETE AND UPLOAD MIB FILES page

6. Similarly, multiple MIB files can be uploaded to the eG manager, one after the other (see Figure 8).

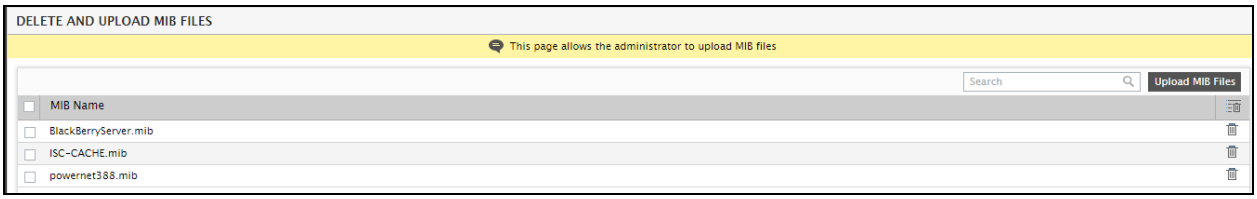

Figure 8: Multiple MIB files uploaded to the eG manager

7. To delete a MIB file, click on the button corresponding to a MIB file in Figure 8. To delete multiple MIB files at one shot, select the check box that precedes each MIB file to mark it for deletion. To mark all MIB files for deletion, click on the check box that precedes the column head **MIB Name** in Figure 8. Then, click on the button corresponding to the column head **MIB Name** to delete the selection.